

# EXHIBIT A

PACIFIC TRIAL ATTORNEYS  
A Professional Corporation  
Scott J. Ferrell, Bar No. 202091  
sferrell@pacifictrialattorneys.com  
4100 Newport Place Drive, Ste. 800  
Newport Beach, CA 92660  
Tel: (949) 706-6464  
Fax: (949) 706-6469

Attorneys for Plaintiff

Electronically FILED by  
Superior Court of California,  
County of Los Angeles  
7/25/2023 2:20 PM  
David W. Slayton,  
Executive Officer/Clerk of Court,  
By J. Nunez, Deputy Clerk

**SUPERIOR COURT FOR THE STATE OF CALIFORNIA**  
**COUNTY OF LOS ANGELES**

SONYA VALENZUELA, individually and on  
behalf of all others similarly situated,

Plaintiff,

v.

MICRON TECHNOLOGY, INC., a Delaware  
corporation d/b/a WWW.CRUCIAL.COM,

Defendant.

Case No. **23STCV17448**

**CLASS ACTION COMPLAINT**

## **INTRODUCTION**

Defendant has secretly installed a collection of surveillance tools on its website at [www.crucial.com](http://www.crucial.com) to identify and “dox” every anonymous visitor. Defendant enables the malware companies to wiretap and eavesdrop on all conversations conducted through the website chat feature, access every visitor’s device, and extract personal data to identify every visitor by name. Defendant and the malware companies then exploit their knowledge of visitors’ identities, habits, and chat topics to bombard visitors with targeted marketing, including unwanted telephone calls and e-mails.

Defendant does all of this without visitors’ effective informed consent. As a result, Defendant has violated numerous laws.

## **JURISDICTION AND VENUE**

1. Defendant is subject to jurisdiction in this state under Penal Code Section 502(j), which provides that a person who causes, by any means, the access of a computer in California from another jurisdiction is deemed to have personally accessed the computer in California. Defendant is also subject to jurisdiction under California’s “long-arm” statute found at California Code of Civil Procedure Section 410.10 because the exercise of jurisdiction over Defendant is not “inconsistent with the Constitution of this state or the United States.”

2. Venue is proper in this County in accordance with California Code of Civil Procedure Section 394(b) because “none of the defendants reside in the state.” As such, venue is proper “in any county that the plaintiff may designate in his or her complaint.”

## **PARTIES**

3. Plaintiff is a resident of California. While physically within California within the past year, Plaintiff visited Defendant’s Website using a smart phone and conducted a brief conversation with an agent of Defendant through the Website’s chat feature. Plaintiff was not advised that the chat was monitored, intercepted, or recorded.

4. Defendant is a Delaware corporation with its principal place of business in Idaho. It sells computer memory and computer data storage products throughout the United States via its

1 website and other distribution channels. Defendant also owns and operates the above-referenced  
2 Website.

### 3 **FACTUAL ALLEGATIONS**

#### 4 **A. The Right to Privacy Has Always Been a Legally Protected Interest in the United States.**

5 5. Since America's founding, privacy has been a legally protected interest at the local,  
6 state, and federal levels. *See Patel v. Facebook, Inc.*, 932 F.3d 1264, 1271–72 (9th Cir. 2019) (quoting  
7 *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016)) (“Privacy rights have long been regarded ‘as  
8 providing a basis for a lawsuit in English or American courts.’”); and *Eichenberger v. ESPN, Inc.*, 876  
9 F.3d 979, 983 (9th Cir. 2017) (“Violations of the right to privacy have long been actionable at  
10 common law.”).

11 6. More specifically, privacy protections against the disclosure of certain kinds of  
12 sensitive personal information are embedded in California statutes and at common law. *See e.g., U.S.*  
13 *Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989) (“The Ninth  
14 Circuit has repeatedly held that privacy intrusions may constitute “concrete injury” for purposes of  
15 Article III standing); *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1041–43 (9th Cir.  
16 2017) (finding “concrete injury” where plaintiffs claimed that unsolicited telemarketing calls “invade  
17 the privacy and disturb the solitude of their recipients”); *In re Facebook, Inc. Internet Tracking Litig.*,  
18 956 F.3d 589, 599 (9th Cir. 2020) (finding “concrete injury” where Facebook allegedly tracked users’  
19 “personally identifiable browsing history” on third party websites); *Patel*, 932 F.3d at 1275 (finding  
20 “concrete injury” where plaintiffs claimed Facebook’s facial-recognition technology violated users’  
21 privacy rights).

22 7. In short, privacy is—and has always been—a legally protected interest in many  
23 contexts, including specifically with regard to sensitive personal information. Thus, a defendant whose  
24 acts or practices violate consumer privacy inflicts an actionable “injury” upon an individual.

#### 25 **B. The Right to Privacy Includes The Right To Online Anonymity.**

26 8. The right to privacy includes the right to anonymity online. *In Re Anonymous Online*  
27 *Speakers*, 661 F.3d 1168 (9th Cir. 2011). Indeed, the “free exchange of ideas on the Internet is driven  
28

1 in large part by the ability of Internet users to communicate anonymously.” *Doe v. 2TheMart.com*  
2 *Inc.*, 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001).

3 9. Consumer expectations regarding privacy reinforce the actionability of these rights.  
4 According to Pew Research Center nearly all Americans believe it is important to (1) be in control of  
5 who can get information about their online activities; (2) to not be tracked online without their  
6 consent; and (3) to be in control of what information is collected about them.

7 10. Accordingly, most people don't want their private online browsing to be associated with  
8 their public offline identities. This is because online anonymity gives the freedom to investigate,  
9 explore, and research without fear of social repercussions. In addition, online anonymity helps prevent  
10 security breaches, surveillance and intrusive web-tracking.

11 **C. The De-Anonymization of Internet Users Poses a Serious Threat to Personal Privacy and**  
12 **the Internet.**

13 11. In simple terms, de-anonymization is a process that involves cross-referencing  
14 anonymized data with “commercially available information” (“CAI”) obtained from grey data markets  
15 to reveal an individual's identity. De-anonymization has been called the “the biggest privacy threat no  
16 one is talking about.”<sup>1</sup>

17 12. As the Director of National Intelligence explained in a January 22, 2022 report  
18 (approved for public release on June 5, 2023) (the “DNI Report”), “the volume and sensitivity of CAI  
19 have expanded in recent years mainly due to the advancement of digital technology, including  
20 location-tracking and other features of smartphones and other electronic devices, and the advertising-  
21 based monetization models that underlie many commercial offerings available on the Internet.”

22 13. The Director of National Intelligence concluded (1) that the existence of these practices  
23 poses a threat to national security since it is available to foreign governments since it “clearly provides  
24 intelligence value,” and (2) that it “raises significant issues related to privacy and civil liberties.”

25 14. The Director of National Intelligence concluded that the “single most important point”  
26 is that the expansion of CAI is “increasingly powerful for intelligence and increasingly sensitive for  
27

28 <sup>1</sup> <https://technoglitx.com/de-anonymization-is-the-biggest-threat-to-privacy-that-no-one-is-talking-about/> (last downloaded July 2023).

individual privacy and civil liberties” such that the Intelligence Community “needs to develop more refined policies to govern its acquisition and treatment.”

**D. Defendant Uses “Identity Resolution” Malware Tools to Access Every Visitor’s Device, Reveal Their Identities, and Publicize Their Personal Information to Its Marketing Partners.**

15. As noted above, internet users have the right to remain anonymous. Nevertheless, some unscrupulous companies sell website owners “identity resolution” malware tools to de-anonymize and track website visitors. Identity resolution is generally defined as “the ability to recognize an individual person, in real-time, by connecting various identifiers from their digital interactions across devices and touchpoints.” See <https://www.fullcontact.com/identity-resolution/> (last downloaded July 2023).

16. Identity resolution requires the collection of “technical markers” and other clues that digital visitors leave when they use the internet, even though most users “are trying to reveal as little information as possible.” See <https://venturebeat.com/ai/what-is-identity-resolution-its-benefits-challenges-and-best-practices/> (last downloaded July 2023). Those “technical markers” include routing information, locally stored data (sometimes called “cookies”), and idiosyncratic behavior of computers. The techniques have grown much more sophisticated over the years, and modern identity resolution algorithms rely upon dozens of types of details and digital footprints. *Id.*

17. In short, identity resolution providers aggregate visitor “touchpoints” containing anonymous identifiers to find links between the anonymous identifiers until the data compiled into a dossier about an anonymous individual can be linked to a specific individual by name, age, address, physical location, and more.

18. The following visual depiction shows an example of how identity resolution providers aggregate dozens of “touchpoints” to identify an anonymous internet user:



19. In the above example, the identity resolution provider has aggregated and analyzed dozens of anonymous “touchpoints” to reveal the following about a previously anonymous internet user, Mary Smith:

- (a) Full name (*Mary Smith*)
- (b) Date of birth (*May 1, 1979*)
- (c) Gender (*female*)
- (d) Home address (*2345 Avenue C, Papillion Nebraska*)
- (e) Marital Status and Family (*Married with two children*)
- (f) E-mail address ([Mary.Smith@gmail.com](mailto:Mary.Smith@gmail.com))
- (g) Personal Cell Phone: *(111) 123-4567*
- (h) Voter Registration Status (*Registered*)
- (i) Interests (*Shopping, Cooking, Traveling, Reading, Science*)
- (j) Employer (*Karen's Fireside, Inc.*)

(k) Title (*Vice President*)

(l) Work Hours (*Daily 9-5*)

20. To identify and “dox” each visitor, Defendant has deployed the following malware tools on its website:

a. **Marketo**: Marketo’s AdBridge Identity Resolution Malware, powered by LiveRamp, allows marketers to achieve true people-based marketing using the world’s largest independent omnichannel identity graph. See <https://direct-launchpoint.marketo.com/launchpoint-labs/marketoliveramp/> (last downloaded July 2023). LiveRamp’s Identity Resolution Malware “resolves disparate identifiers into individuals or households across digital, mobile, and connected TV into a unified view of the customer by “connecting consumers’ offline and online journeys across various touchpoints and devices.” See <https://docs.liveramp.com/identity/en/rampid-identity-resolution.html> (last downloaded July 2023).

b. **Bizrate Insights**: Bizrate’s Identity Resolution Malware uses both qualitative and quantitative metrics to de-anonymize website visitors so users can “get know your customers on a human level. See <https://www.bizrateinsights.com/marketing/> (last downloaded July 2023).

21. Within the statute of limitations period, Plaintiff visited Defendant’s website and communicated with Defendant via Defendant’s chat feature. As a result of Defendant’s use of identity resolution malware and intrusion onto Plaintiff’s device, Defendant: (1) obtained the IP address of Plaintiff; (2) identified Plaintiff’s name, location, e-mail, browsing history, and other personal information; and (3) embedded Plaintiff’s identity into the malware companies’ extensive “gray market CAI” database, which the malware companies share virally with other companies that purchase their products.

22. As a result of Defendant’s wrongful conduct: (1) Plaintiff has been de-anonymized and Plaintiff’s personal information has been added to an extensive malware database; (2) Plaintiff has been bombarded with targeted advertising, e-mails, and telephone calls; (3) Plaintiff can no longer surf the web anonymously; and (4) Plaintiff has been exposed to heightened risk of identity theft.



23. In short, Defendant has deprived Plaintiff of numerous important privacy rights protected under California common law and statutes. Defendant's conduct amounts to "doxing by deanonymization" and robs Plaintiff of anonymity and obscurity. As a result, it is now easier for other companies to obtain other types of identity knowledge about Plaintiff and subject Plaintiff to further doxing. See *Doxing: A Conceptual Analysis, Ethics and Information Technology* (Volume 18, pages 199–210 (2016)).

**E. Defendant's Further Violation of California Invasion of Privacy Act.**

24. In addition to de-anonymizing and doxing class members, Defendant also allows a malware company to wiretap and eavesdrop upon class member communications through the website chat feature in violation of California law.

25. CIPA prohibits both wiretapping and eavesdropping of electronic communications without the consent of all parties to the communication. "[T]he right to control the nature and extent of the firsthand dissemination of [one's] statements" is viewed by the California Supreme Court "as critical to the purposes of Section 631[.]" *Javier v. Assurance IQ, LLC*, 2023 WL 114225, at \*6 (N.D. Cal. Jan. 5, 2023) (Breyer, J.) (quoting *Ribas v. Clark*, 38 Cal. 3d 355, 361 (1985)); *Ribas*, 38 Cal. 3d at 360-61 ("a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device"). "[U]nder Section 631, it has always mattered who is holding the tape recorder[.]" *Javier*, 2023 WL 114225, at \*6. Compliance with CIPA is easy, and most website operators comply by conspicuously warning visitors if their conversations are being recorded, intercepted, or eavesdropped upon.

26. Unlike most companies, Defendant *ignores* CIPA. Instead, Defendant enables and allows the third parties to eavesdrop on all such conversations. Why? Because, as one industry expert notes, "*Live chat transcripts are the gold mines of customer service. At your fingertips, you have valuable customer insight to make informed business decisions. . . . When people are chatting, you have direct access to their exact pain points.*"). See <https://www.ravience.co/post/improve-marketing-roi-live-chat-transcripts> (last visited July 2023) (emphasis added).

27. To enable the eavesdropping, Defendant allowed a company called Salesforce to

1 covertly embed code into Defendant's chat feature.

2 28. The secret code is a type of automatic routing software that automatically acquires and  
3 transmits user chat communications to Salesforce without any active input from Defendant's  
4 employees. The code enables and allows Salesforce to secretly intercept in real time, eavesdrop upon,  
5 and store transcripts of Defendant's chat communications with unsuspecting website visitors – even  
6 when such conversations are private and personal. Defendant neither informs visitors of this conduct  
7 nor obtains their consent to these intrusions.

8 29. One might reasonably wonder why Salesforce would be interested in intercepting and  
9 recording the website chat interactions between Defendant and unsuspecting visitors to Defendant's  
10 Website. As shown below, it all about money.

11 30. Salesforce's chat software is easily "integrated" with Meta, Inc.'s subsidiaries like  
12 Facebook and WhatsApp. (Integration allows various software sub-systems to share data to operate as  
13 a unified system). According to Bloomberg.com, this is all part of Meta's secret "***plan to profit from***  
14 ***private chats.***" As Bloomberg explained, Meta's software integration "*can manage customer*  
15 *messages from multiple services on one central dashboard. That's central to Meta's plan to make*  
16 *money off of its two messaging apps, WhatsApp and Messenger.*" See  
17 [https://www.bloomberg.com/news/articles/2022-02-15/meta-closes-1-billion-kustomer-deal-after-](https://www.bloomberg.com/news/articles/2022-02-15/meta-closes-1-billion-kustomer-deal-after-regulatory-review)  
18 [regulatory-review](https://www.bloomberg.com/news/articles/2022-02-15/meta-closes-1-billion-kustomer-deal-after-regulatory-review) (last downloaded March 2023).

19 31. So how does it work? ***First***, Meta identifies "user interests" by monitoring a collection  
20 of "offsite" user activity such as website visits and interactions (including private chat  
21 communications between Defendant and visitors) by "integrating" its software with Salesforce and the  
22 Identity Resolution Malware Companies identified above. ***Second***, Meta and the Identity Resolution  
23 Malware Companies generate revenue based on their ability to identify anonymous internet users,  
24 along with their habits, preferences, and interests. ***Third and finally***, after the chat transcripts  
25 intercepted by Salesforce are provided to Meta and the Third Party Identity Resolution Malware  
26 Companies, visitors are bombarded with targeted advertising, e-mails, and telephone calls.

27 32. Through the preceding acts, Meta's boasts that it will "Transform your support center  
28 into a profit generator by bulk messaging specific customer segments based on your unique data...to

1 reengage dissatisfied customers.” See <https://www.kustomer.com/product/customer-service/> (last  
2 downloaded May 16, 2023 (link preserved but since disabled).

3 33. Salesforce does more than merely provide a storage function for Defendant regarding  
4 Website users’ chat communications with Defendant. As shown above, Salesforce uses its record of  
5 Website users’ interaction with Defendant’s chat feature to enable targeted marketing by Defendant  
6 and the Identity Resolution Malware Companies.

7 34. Indeed, all of the schemers – Defendant, Salesforce, Meta, and the Identity Resolution  
8 Malware Companies – all profit from secretly exploiting their ability to identify anonymous  
9 individuals who have visited Defendant’s website. How? Because “*Targeted advertising allows*  
10 *brands to send different messaging to different consumers based on what the brand knows about the*  
11 *customer. The better a brand can demonstrate that it understands what its customers want and need,*  
12 *the more likely customers respond to advertising and engage with the brand. . . .Social media*  
13 *targeting helps brands leverage consumers’ behavior on the web, search engines, and social media*  
14 *sites to present ads that reflect consumer interests.”*<sup>2</sup>

15 35. Plaintiff visited Defendant’s Website using a smart phone (a cellular telephone with  
16 integrated computers to enable web browsing). As such, Plaintiff conversations through the website  
17 chat feature was transmitted from “cellular radio telephony” as defined by CIPA.

18 36. By definition, Defendant’s chat communications from its Website are transmitted to  
19 website visitors by either cellular telephony or landline telephony. See  
20 <https://www.britannica.com/technology/Internet> (“How does the Internet work?”) (“*The Internet works*  
21 *through a series of networks that connect devices around the world through telephone lines.*”) (last  
22 visited May 16, 2023) (emphasis added).

23 37. Defendant did not inform Class members that Defendant was secretly allowing, aiding,  
24 and abetting Salesforce to intercept and eavesdrop on the conversations during transmission, or that  
25 Salesforce provided data from such transcripts to Meta and the malware companies through  
26 “integration” with Meta software.

27 <sup>2</sup> See [https://www.adroll.com/blog/what-is-targeted-](https://www.adroll.com/blog/what-is-targeted-advertising#:~:text=Targeted%20advertising%20allows%20brands%20to,and%20engage%20with%20the%20brand)  
28 [advertising#:~:text=Targeted%20advertising%20allows%20brands%20to,and%20engage%20with%20the%20brand](https://www.adroll.com/blog/what-is-targeted-advertising#:~:text=Targeted%20advertising%20allows%20brands%20to,and%20engage%20with%20the%20brand) (last visited July 2023).

38. Defendant did not obtain class members' effective consent for the preceding intrusions, nor were class members aware of Defendant's conduct.

**CLASS ALLEGATIONS**

39. Plaintiff brings this action individually and on behalf of all others similarly situated (the "Class") defined as follows:

**All persons within the state of California who within the statute of limitations period: (1) visited Defendant's website; and (2) were exposed to the wrongful conduct described above.**

40. NUMEROSITY: Plaintiff does not know the number of Class members but believes the number to be in the tens of thousands. The exact identities of Class members may be ascertained by the records maintained by Defendant.

41. COMMONALITY: Common questions of fact and law exist as to all Class members, and predominate over any questions affecting only individual members of the Class. Such common legal and factual questions, which do not vary between Class members, and which may be determined without reference to the individual circumstances of any Class member, include but are not limited to the following:

- a. Whether Defendant engaged in the wrongful conduct described above;
- b. Whether Plaintiff and Class members are entitled to statutory penalties; and
- c. Whether Class members are entitled to injunctive relief.

42. TYPICALITY: As a person who visited Defendant's Website, whose privacy was invaded and whose electronic communication was recorded, intercepted and eavesdropped upon, Plaintiff is asserting claims that are typical of the Class.

43. ADEQUACY: Plaintiff will fairly and adequately protect the interests of the members of The Class. Plaintiff has retained attorneys experienced in the class action litigation. All individuals with interests that are actually or potentially adverse to or in conflict with the class or whose inclusion would otherwise be improper are excluded.

44. SUPERIORITY: A class action is superior to other available methods of adjudication because individual litigation of the claims of all Class members is impracticable and inefficient. Even

1 if every Class member could afford individual litigation, the court system could not. It would be  
2 unduly burdensome to the courts in which individual litigation of numerous cases would proceed.

3 **FIRST CAUSE OF ACTION**

4 **Violations of the California Invasion of Privacy Act**

5 **Cal. Penal Code § 631(a)**

6 45. “Any person who, by means of any machine, instrument, or contrivance, or in any other  
7 manner, [i] intentionally taps, or makes any unauthorized connection, whether physically, electrically,  
8 acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument,  
9 including the wire, line, cable, or instrument of any internal telephonic communication system, or [ii]  
10 who willfully and without the consent of all parties to the communication, or in any unauthorized  
11 manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or  
12 communication while the same is in transit or passing over any wire, line, or cable, or is being sent  
13 from, or received at any place within this state; or [iii] who uses, or attempts to use, in any manner, or  
14 for any purpose, or to communicate in any way, any information so obtained, or [iv] who aids, agrees  
15 with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be  
16 done any of the acts or things mentioned above in this section, is punishable by a fine . . . .” *Yoon v.*  
17 *Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1080 (C.D. Cal. 2021) (Holcomb, J.) (line breaks and  
18 headings of clauses added for ease of reference) (quoting Cal. Penal Code § 631(a)).

19 46. Section 631 of the California Penal Code applies to internet communications and thus  
20 applies to Plaintiff’s and the Class’s electronic communications with Defendant’s Website. “Though  
21 written in terms of wiretapping, Section 631(a) applies to Internet communications. It  
22 makes liable anyone who ‘reads, or attempts to read, or to learn the contents’ of a communication  
23 ‘without the consent of all parties to the communication.’” *Javier v. Assurance IQ, LLC*, 2022 WL  
24 1744107, at \*1 (9th Cir. 2022); *Yoon*, 549 F. Supp. 3d at 1080 (“Courts agree ... that CIPA § 631  
25 applies to communications conducted over the internet.”) (citing *Matera v. Google Inc.*, 2016 WL  
26 8200619, at \*18 (N.D. Cal. Aug. 12, 2016) (Koh, J.) (holding that second clause of section 631(a)  
27 “encompasses email communications, which pass over wires, lines, or cables”)); *In re Google Inc.*  
28 *Gmail Litig.*, 2013 WL 5423918, at \*21 (N.D. Cal. Sept. 26, 2013) (Koh, J.) (“the Court finds that

1 section 631 of CIPA applies to emails”); *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797,  
2 826 (N.D. Cal. 2020) (Labson Freeman, J.).

3 47. The software embedded on Defendant’s Website to record and eavesdrop upon the  
4 Class’s communications qualifies as a “machine, instrument, contrivance, or ... other manner” used to  
5 engage in the prohibited conduct alleged herein. *See In re Facebook Internet Tracking Litig.*, 140 F.  
6 Supp. 3d 922, 937 (N.D. Cal. 2015) (stating that “*it is undeniable that a computer may qualify as a*  
7 *‘machine’*” within the meaning of section 631(a)) (emphasis added), *aff’d in part and rev’d in part on*  
8 *other grounds*, 956 F.3d 589 (9th Cir. 2020).

9 48. At all relevant times, Defendant intentionally caused the internet communication  
10 between Plaintiff and Class Members with Defendant’s Website to be recorded. Defendant also aided  
11 and abetted, agreed with, employed, or conspired with Salesforce to wiretap and/or eavesdrop upon  
12 such conversations during transmission and in real time by voluntarily embedding the software code.

13 49. Defendant knows that Salesforce captures the electronic communications of visitors to  
14 Defendant’s Website, and pays Salesforce to conduct these activities.

15 50. Plaintiff and Class Members did not expressly or impliedly consent to any of  
16 Defendant’s actions.

17 51. A line of materially identical cases is pending in the Central District of California  
18 before the Honorable Sunshine S. Sykes. In the lead case, Judge Sykes held held that the above-  
19 described allegations state viable claims for violations of section 631(a) of CIPA. *See Byars v. The*  
20 *Goodyear Tire & Rubber Co.*, No. 5:22-cv-01358-SSS-KKx, 2023 WL 1788553, at \*4 (C.D. Cal. Feb.  
21 3, 2023) (Sykes, J.) (“*Byars contends that Goodyear, using a third-party service, “intercepts in real*  
22 *time” a website visitors’ chat conversation. . . . Byars alleges that, using the chat conversation,*  
23 *website visitors share sensitive personal information. . . . Because Byars has pled sufficient facts to*  
24 *show the contents of the communications and that the communications were intercepted, Byars has*  
25 *sufficiently stated a claim under § 631(a).*”) (emphasis added).

26 52. Defendant’s conduct constitutes numerous discrete violations of Cal. Penal Code §  
27 631(a), entitling Plaintiff and/or Class Members to injunctive relief and statutory damages.

28 **SECOND CAUSE OF ACTION**

**Violations of the California Invasion of Privacy Act**

**Cal. Penal Code § 632.7**

53. Section 632.7 of California’s Penal Code imposes liability upon anyone “who, without the consent of all parties to a communication, intercepts or receives and intentionally records, or assists in the interception or reception and intentional recordation of, a communication transmitted between two cellular radio telephones, a cellular radio telephone and a landline telephone, two cordless telephones, a cordless telephone and a landline telephone, or a cordless telephone and a cellular radio telephone.”

54. Plaintiff and the class members communicated with Defendant using telephony subject to the mandates and prohibitions of Section 632.7.

55. Defendant’s communication from the chat feature on its Website is transmitted via telephony subject to the mandates and prohibitions of Section 632.7.

56. As set forth above, Defendant recorded telephony communication without the consent of all parties to the communication in violation of Section 632.7.

57. As set forth above, Defendant also aided and abetted a third party in the interception, reception, and/or intentional recordation of telephony communication in violation of Section 632.7.

58. In the lead pending federal case, Judge Sykes held that the above-described allegations state viable claims for violations of section 632.7 of CIPA. *See Byars v. The Goodyear Tire & Rubber Co.*, No. 5:22-cv-01358, 2023 WL 1788553, at \*5 (C.D. Cal. Feb. 3, 2023) (Sykes, J.) (“*Byars’ alleged communication with Goodyear occurred via Goodyear’s chat feature on its website. Byars accessed Goodyear’s website using her smartphone. As smartphones are cellular phones with web capabilities, Byars’ smartphone falls within the cellular phone category. . . . Because Byars’ contends that users of Goodyear’s website “share highly sensitive personal data” via Goodyear’s chat feature, Byars has sufficiently alleged that website users had a reasonable expectation of privacy and therefore the communications fall within the scope of § 632.7.*”) (emphasis added and internal citations omitted).

59. Defendant’s conduct constitutes numerous discrete violations of Cal. Penal Code § 632.7, entitling Plaintiff and/or Class members to injunctive relief and statutory damages.

**THIRD CAUSE OF ACTION**



**CALIFORNIA UNAUTHORIZED ACCESS TO COMPUTER DATA ACT**

**PENAL CODE SECTION 502**

60. The California Unauthorized Access to Computer Data Act (the “CUCA”) makes it unlawful for parties to obtain data from a computer user outside of the scope of the user’s authorization.

61. Specifically, Penal Code Section 502(c) imposes liability on any entity that “knowingly accesses and without permission” (1) uses any computer data, in order to “wrongfully control or obtain” computer data, or (2) “makes use of any data from a computer...”

62. CUCA provides a private right of action for compensatory damages, punitive damages, and attorneys’ fees to any individual harmed by its violation. *See Facebook, Inc. v. Power Ventures, Inc.*, 2012 WL 542586 (N.D. Cal. Feb. 16, 2012).

63. By knowingly installing the Identity Resolution Malware to access class member devices and extract their personal information, Defendant violated CUCA. *See United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2015) (violation of CUCA to access a device and use data improperly); and *Gilbert v. City of Sunnyvale* (2005) 130 Cal. App. 4th 1264, 1281 (accessing and without permission making use of any data from a computer system) violates CUCA.

**FOURTH CAUSE OF ACTION**

**CALIFORNIA INVASION OF PRIVACY**

64. Article I, § 1 of the California Constitution provides, “All people are by nature free and independent and have inalienable rights. Among those are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.”

65. The phrase “and privacy” was added by an initiative adopted by California voters on November 7, 1972 (the Privacy Initiative). The Privacy Initiative created a private right of action against nongovernmental entities for invasions of privacy.

66. The California Supreme Court has explained that one of the principal “mischiefs” to which the Privacy Initiative was directed was “the overbroad collection and retention of unnecessary



1 personal information by government and business interests.” *White v. Davis*, 13 Cal.3d 757, 775 (Cal.  
2 1975).

3 67. Defendant’s conduct in secretly accessing class member devices, gathering highly  
4 personal details about them and their browsing history, and sharing that information with malware  
5 companies amounts to doxing and violates class members’ rights to privacy.

6 68. Defendant assisted the malware companies to create etailed dossiers of class members  
7 and then share it with and sell it to numerous other companies.

8 69. Class members have the right to privacy in their web-browsing history; in how personal  
9 information is going to be used; in the right to withhold and not disclose personal information; and all  
10 statutory privacy rights codified under federal and California law.

11 70. Defendant has intruded on these privacy interests.

12 71. Defendant’s actions constitute a serious invasion of privacy in that they violate several  
13 state laws; disclosed sensitive personal information to third parties; and facilitated the disclosure of  
14 class member information by third parties who did not have legal access to their personal information.

15 72. Defendant acted with oppression, fraud, or malice.

16 73. Class members have been damaged by Defendant’s invasion of privacy and are entitled  
17 to just compensation in the form of actual and punitive damages.

18 **FIFTH CAUSE OF ACTION**

19 **INTRUSION UPON SECLUSION**

20 74. A claim for intrusion upon seclusion requires (1) intrusion into a private place,  
21 conversation, or matter; and (2) in a manner highly offensive to a reasonable person.

22 75. Defendant intentionally intruded upon class members’ solitude and seclusion by (1)  
23 secretly accessing their devices to install identity resolution malware without their knowledge or  
24 permission; and (2) mining their personal data and sharing it with malware companies.

25 76. As set forth above, the right to online privacy is both actionable and expected by  
26 consumers. As such, Defendant’s brazen de-anonymization of class members was highly offensive to  
27 all reasonable persons.

28 77. None of Defendant’s actions were authorized.

1 78. Defendant violated state criminal and civil laws designed to protect individual privacy  
2 and against theft.

3 79. Defendant has acted with oppression, fraud, or malice.

4 80. Class members are entitled to just compensation in the form of actual damages and  
5 punitive damages under this cause of action.


6 **PRAYER FOR RELIEF**

7 WHEREFORE, Plaintiff prays for the following relief against Defendant:

- 8 1. An order certifying the Class, naming Plaintiff as the representative of the Class and  
9 Plaintiff's attorneys as Class counsel;  
10 2. An order declaring Defendant's conduct violates the above-referenced laws;  
11 3. An order of judgment in favor of Plaintiff and the Class and against Defendant on the  
12 causes of action asserted herein;  
13 4. An order enjoining Defendant's conduct as alleged herein and any other injunctive  
14 relief that the Court finds proper;  
15 5. Statutory, actual, and punitive damages;  
16 6. Reasonable attorneys' fees and costs; and  
17 7. All other relief that would be just and proper as a matter of law or equity;

18  
19 Dated: July 25, 2023

PACIFIC TRIAL ATTORNEYS, APC

20 By:   
21 Scott. J. Ferrell  
22 Attorneys for Plaintiff  
23  
24  
25  
26  
27  
28